Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Mission Assurance Analysis Protocol (MAAP)

Sponsored by the U.S. Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Mission Assurance Analysis Protocol (MAAP)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

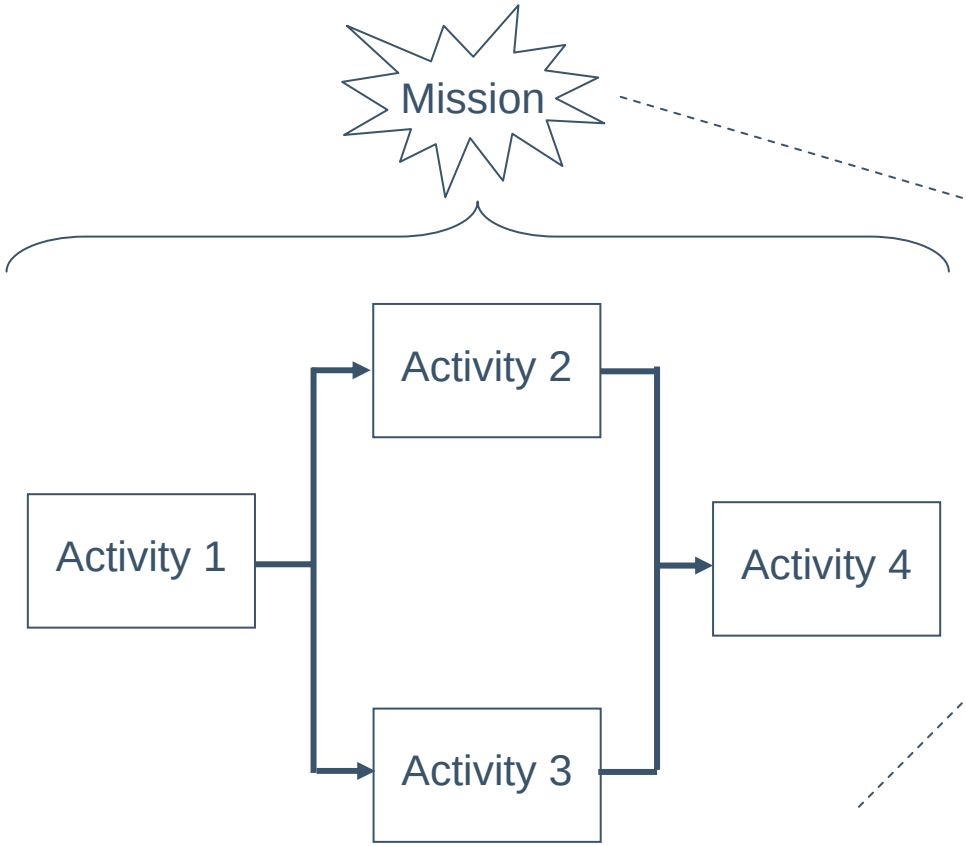
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

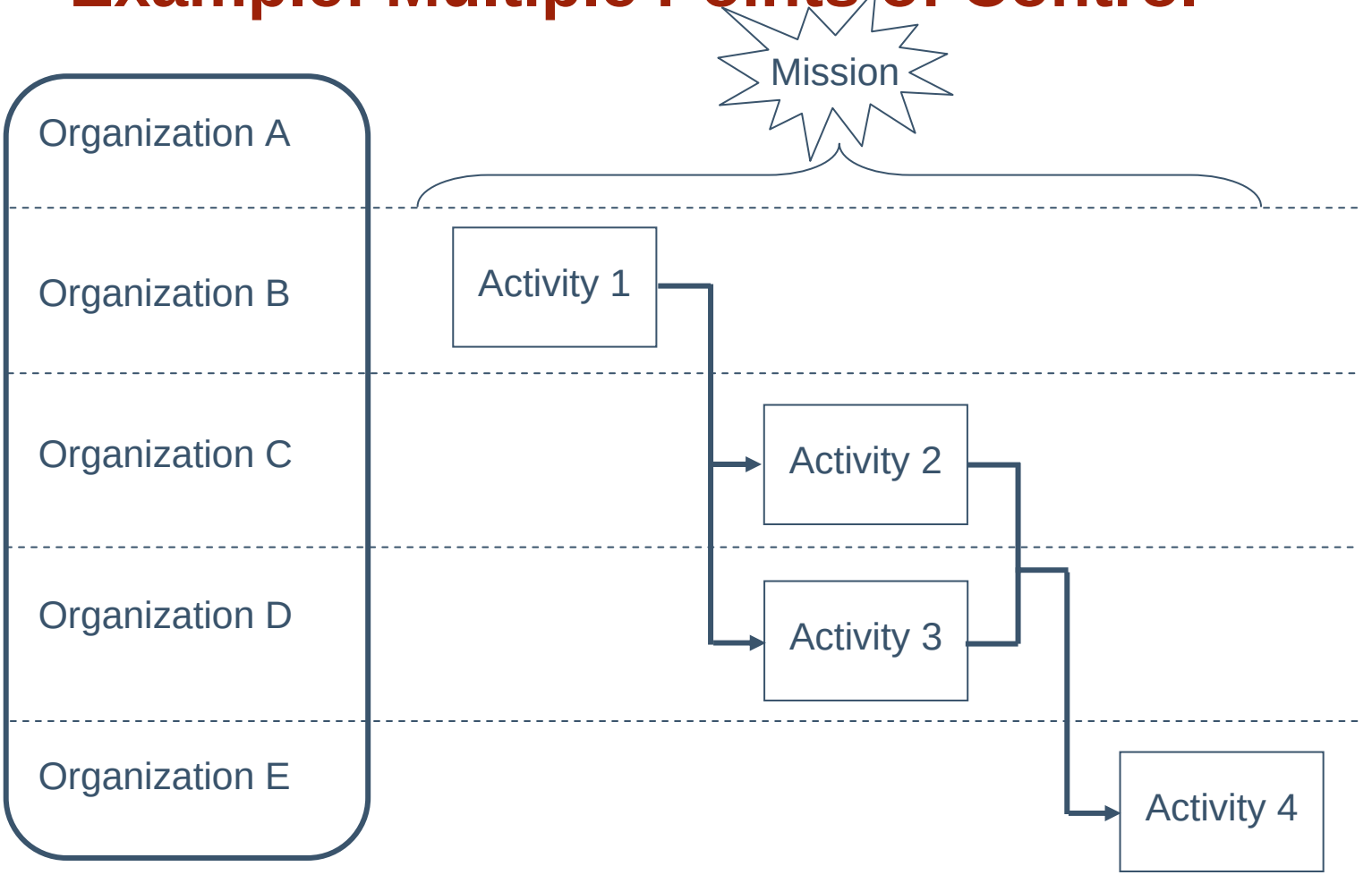
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**19**	

Example: Single Point of Control

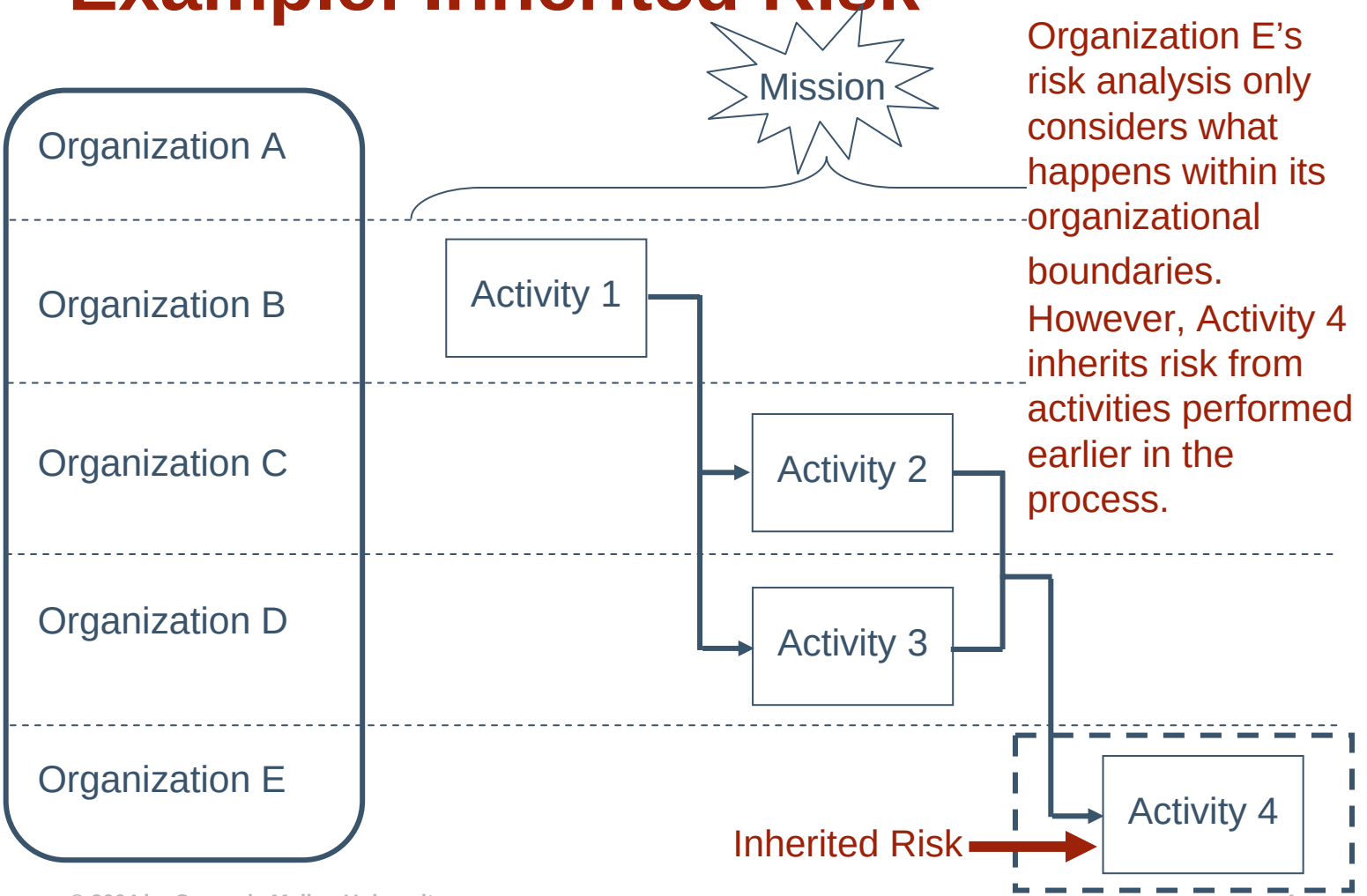


Single point of management control oversees execution of all activities.

Example: Multiple Points of Control



Example: Inherited Risk



Organization E's risk analysis only considers what happens within its organizational boundaries. However, Activity 4 inherits risk from activities performed earlier in the process.

Key Premise

Most risk analysis techniques focus on a single entity (e.g., enterprise, system). These techniques

- are effective at handling environments where management control is centralized
- do not readily scale to environments where management control is distributed

Distributed management of processes and technologies is now commonplace.

New techniques are needed to handle the complexity inherent in distributed environments.

Definitions

Mission is the set of objectives being pursued by a person or group.

Risk is the possibility of suffering harm or loss.

Operational risk is the possibility of direct or indirect loss resulting from failed or inadequate internal processes or from failures caused by people, technology, or external events.

Operational risk tolerance is the maximum overall exposure to operational risk that will be accepted.

Operational Risk Analysis Issues

Analysis of operational risk in distributed environments is often incomplete.

- Some sources of operational risk are excluded from the analysis.
- Interrelationships and dependencies among sources of operational risk are not typically established.
- The potential impact of a risk is often difficult to characterize in complex operational environments.

Operational Risk Management Issues

Management of operational risk in distributed environments is often ineffective.

- Incomplete analysis of operational risk can lead to poor management decisions.
- Operational risk tolerance is not uniform across functional boundaries.
- There are insufficient means for communicating operational risks across functional boundaries.
- Ownership of complex operational risks can be ambiguous.

Mission Assurance

Mission assurance is taking due care to reduce operational risk to the mission to an acceptable level.

Analyzing Mission Assurance - 1

Set the scope of the analysis according to the mission being pursued.

Define and document an interrelated process model for achieving the mission.

- Identify the sequence of all value-added activities that must be performed when working toward the mission.
- Identify the actors responsible for performing each activity.

Establish criteria for measuring operational risk.

Define the tolerance for operational risk.

Analyzing Mission Assurance - 2

Select tools and techniques for data gathering and analysis.

Collect operational risk data.

Analyze operational risk to the mission.

Take action to reduce operational risk to the mission within the defined tolerance.

Sources of Operational Risk

Mission

Design

Execution

Environment

Event

Security and Mission Assurance

The security attributes for information are derived from the performance attributes of work processes.

The tolerance for operational risk establishes the criteria against which security risk must be evaluated.

Security processes are work processes. Operational risk to security processes must be managed in the same way it is managed in other work process.

Mission Assurance Analysis Protocol (MAAP)

Defines a set of objects, rules, and heuristics used to model and analyze processes and systems

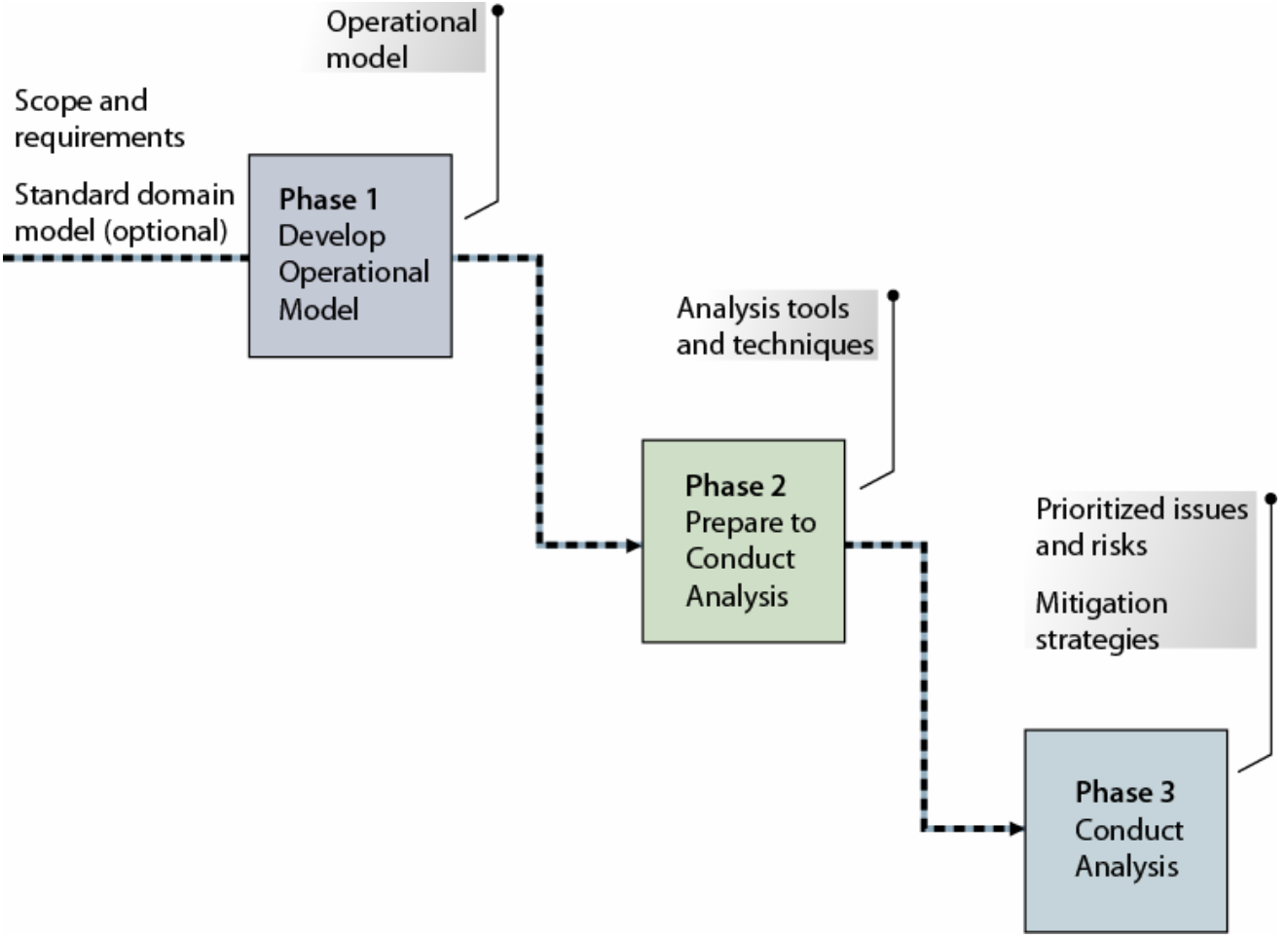
Provides an integrated view of operational risk

Can be tailored to many different domains

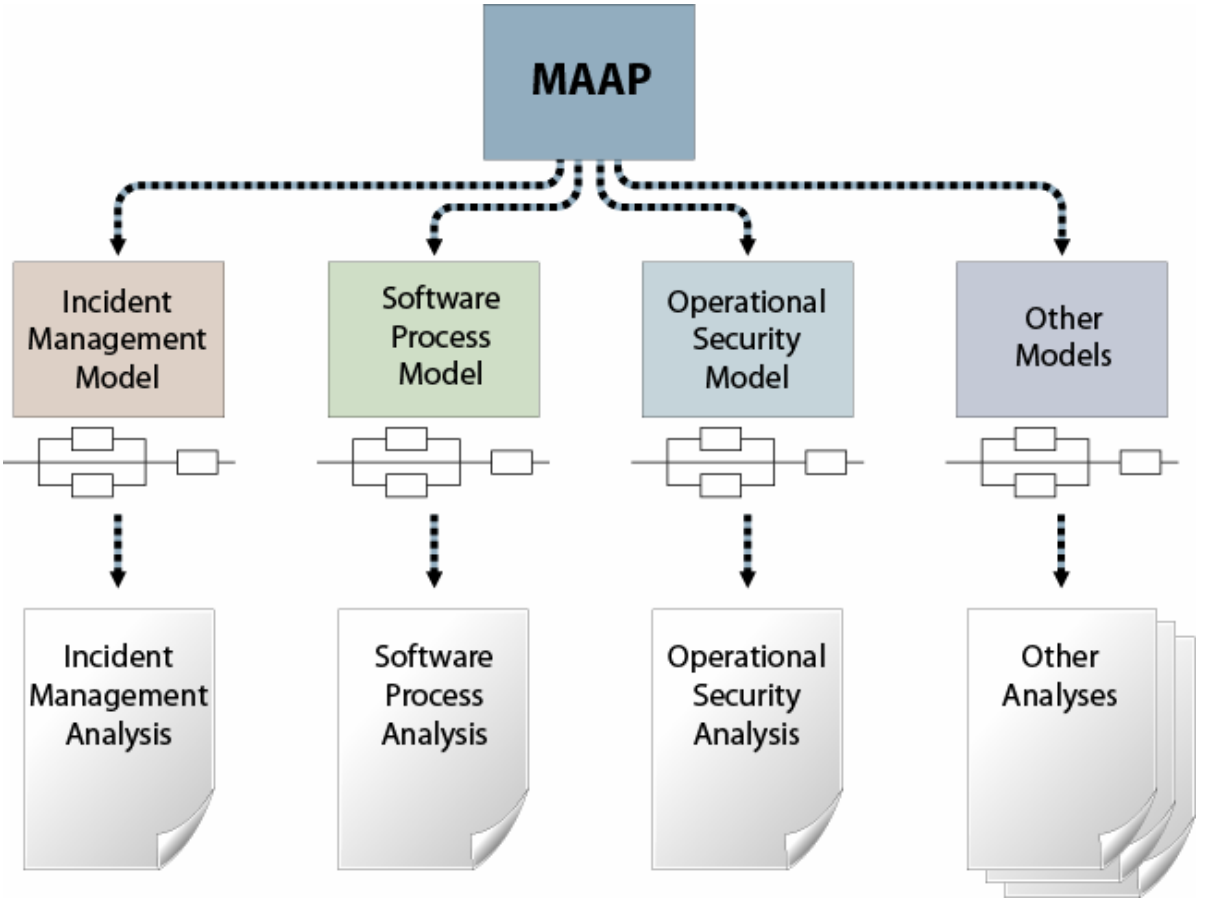
Focuses on assuring the completion of defined missions

Addresses operational risk analysis issues

Implementing MAAP



A Common Basis for Analysis



Types of Analysis

MAAP allows for different types of analysis based on the nature of the problems being solved.

- gap analysis
- qualitative analysis
- quantitative analysis

Proposed Development

MAAP Definition and Description

MAAP Toolkit

MAAP Project Status

First pilot analyzing risk to an incident management capability is underway.

- The operational model has been developed.
- Analysis activities are beginning.

Currently looking for a second pilot in another domain.

- software assurance
- operational security
- unique problems (e.g., operating weapons systems, critical infrastructure)
- complex missions requiring a comprehensive risk analysis